



TITLE:

# ON 2-EXTENSIONS WITH RESTRICTED RAMIFICATION (Algebraic number theory and related topics)

AUTHOR(S):

Vogel, Denis

---

CITATION:

Vogel, Denis. ON 2-EXTENSIONS WITH RESTRICTED RAMIFICATION (Algebraic number theory and related topics). 数理解析研究所講究録 2005, 1451: 233-236

ISSUE DATE:

2005-10

URL:

<http://hdl.handle.net/2433/47741>

RIGHT:

# ON 2-EXTENSIONS WITH RESTRICTED RAMIFICATION

DENIS VOGEL

ABSTRACT. We study the connection between Massey products and relations in pro- $p$ -groups and give an arithmetical example related to the 2-class field tower of quadratic number fields.

## 1. MASSEY PRODUCTS AND RELATIONS IN PRO- $p$ -GROUPS

In this section we generalize the well-known connection between the cup product in the cohomology of pro- $p$ -groups and presentations of pro- $p$ -groups in terms of generators and relations.

Let  $p$  be a prime number and  $G$  a finitely generated pro- $p$ -group. In the following we will make use of the cohomology groups  $H^i(G, \mathbb{Z}/p\mathbb{Z})$ , and for simplicity we will denote them by  $H^i(G)$ . We set  $n = \dim_{\mathbb{Z}/p\mathbb{Z}} H^1(G)$ . It is well-known that this is the generator rank of  $G$ . Let

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

be a minimal presentation of  $G$ , where  $F$  is a free pro- $p$ -group on generators  $x_1, \dots, x_n$ . Using the Hochschild-Serre spectral sequence we obtain the exact sequence

$$0 \longrightarrow H^1(G) \xrightarrow{\text{inf}} H^1(F) \xrightarrow{\text{res}} H^1(R)^G \xrightarrow{\text{tg}} H^2(G) \longrightarrow 0.$$

By the minimality of the above presentation it follows that the inflation map

$$\text{inf} : H^1(G) \rightarrow H^1(F)$$

is an isomorphism by which will identify both groups in the following. In particular, also the transgression map

$$\text{tg} : H^1(R)^G \rightarrow H^2(G)$$

is an isomorphism. For each  $\rho \in R$  we have the trace map

$$\text{tr}_\rho : H^2(G) \rightarrow \mathbb{Z}/p\mathbb{Z}, \quad \phi \mapsto (\text{tg}^{-1} \phi)(\rho).$$

Let  $I$  be the kernel of the augmentation map  $\mathbb{F}_p[[F]] \rightarrow \mathbb{F}_p$  where  $\mathbb{F}_p[[F]]$  denotes the complete group algebra of  $F$  over  $\mathbb{F}_p$ . Setting

$$F_{(m)} = \{f \in F \mid f - 1 \in I^m\}$$

we have a filtration on  $F$ , the so-called Zassenhaus filtration. It is well known that the cup product pairing

$$H^1(G) \times H^1(G) \xrightarrow{\cup} H^2(G)$$

yields some information on  $R$ : If  $\chi_1, \dots, \chi_n$  denotes the dual basis of  $H^1(F) = \text{Hom}(F, \mathbb{Z}/p\mathbb{Z})$  to  $x_1, \dots, x_n$  then for each  $\rho \in R$  we have

$$\rho \equiv \prod_{k=1}^n x_k^{pb_{kk}} \prod_{1 \leq k < l \leq n} (x_k, x_l)^{b_{kl}} \pmod{F_{(3)}}$$

(here  $(x_k, x_l)$  is the commutator  $x_k^{-1}x_l^{-1}x_kx_l$ ), with

$$\text{tr}_\rho(\chi_k \cup \chi_l) = -b_{kl}.$$

We are going to study what happens if the cup product is trivial. In this case we have triple Massey products, which are defined as follows. Let  $u_1, u_2, u_3 \in H^1(G)$  with  $u_1 \cup u_2 = 0$ ,  $u_2 \cup u_3 = 0$ . Then there exist 1-cochains  $u_{12}, u_{23}$ , such that on the level of 2-cochains we have

$$u_1 \cup u_2 = \partial u_{12}, \quad u_2 \cup u_3 = \partial u_{23},$$

and we set

$$\langle u_1, u_2, u_3 \rangle = [u_1 \cup u_{23} + u_{12} \cup u_3] \in H^2(G),$$

where  $[\cdot]$  denotes the cohomology class of the corresponding cocycle. We remark that  $\langle u_1, u_2, u_3 \rangle$  is independent of the choices we made. Generalizing this, we can define Massey products  $\langle u_1, \dots, u_m \rangle$  of length  $m$  for  $u_1, \dots, u_m \in H^1(G)$  ([Mo], [Vo]), in general, however,  $\langle u_1, \dots, u_m \rangle$  lies in some quotient of  $H^2(G)$ . We give a criterion when  $\langle u_1, \dots, u_m \rangle$  lies inside  $H^2(G)$  and calculate  $\text{tr}_\rho \langle u_1, \dots, u_m \rangle$  in this case. In order to do so, we need the notations of the Fox differential calculus. If  $\mathbb{Z}_p[[F]]$  denotes the complete group algebra of  $F$  over  $\mathbb{Z}_p$  and  $\psi : \mathbb{Z}_p[[F]] \rightarrow \mathbb{Z}_p$  the augmentation map, then for each  $i = 1, \dots, n$  there exist uniquely determined maps

$$\frac{\partial}{\partial x_i} : \mathbb{Z}_p[[F]] \rightarrow \mathbb{Z}_p[[F]],$$

the so-called free derivatives, such that the equation

$$\alpha = \psi(\alpha)1_{\mathbb{Z}_p[[F]]} + \sum_{i=1}^n \frac{\partial \alpha}{\partial x_i} (x_i - 1)$$

holds for each  $\alpha \in \mathbb{Z}_p[[F]]$ . For  $1 \leq i_1, \dots, i_m \leq n$  we define

$$\varepsilon_{(i_1, \dots, i_m)} : F \rightarrow \mathbb{Z}_p, \quad f \mapsto \psi \left( \frac{\partial^m f}{\partial x_{i_1} \cdots \partial x_{i_m}} \right) \pmod{p}.$$

We have the following theorem (see [Mo], [Vo]).

**Theorem 1.1.**  *$R$  is contained in  $F_{(m)}$  if and only if all Massey products up to length  $m-1$  are trivial. In this case all Massey products of length  $m$  are inside  $H^2(G)$ , and for  $u_1, \dots, u_m \in H^1(G)$ ,  $\rho \in R$  we have*

$$\text{tr}_\rho \langle u_1, \dots, u_m \rangle = (-1)^{m-1} \sum_{1 \leq i_1, \dots, i_m \leq n} u_1(x_{i_1}) \cdots u_m(x_{i_m}) \varepsilon_{(i_1, \dots, i_m)}(\rho).$$

In particular

$$\text{tr}_\rho \langle \chi_{i_1}, \dots, \chi_{i_m} \rangle = (-1)^{m-1} \varepsilon_{(i_1, \dots, i_m)}(\rho)$$

For  $\rho \in F_{(m)}$  the  $\varepsilon_{(i_1, \dots, i_m)}(\rho)$  are intimately connected to the image of  $\rho$  in  $F_{(m)}/F_{(m+1)}$ . We give the following example.

**Example 1.2.** If  $\rho \in F_{(3)}$  and  $p \neq 3$  then

$$f \equiv \prod_{\substack{1 \leq k < l \leq n \\ m \leq l}} ((x_k, x_l), x_m)^{p - \varepsilon(l, k, m)(f)} \prod_{1 \leq k < l \leq n} ((x_k, x_l), x_l)^{\varepsilon(k, l, l)(f)} \pmod{F_{(4)}}.$$

## 2. ON THE 2-CLASS FIELD TOWER OF IMAGINARY QUADRATIC NUMBER FIELDS

In this section we study an example of a triple Massey product coming from number theory. For this purpose we consider the relation structure of the 2-class field tower of an imaginary quadratic number field.

Let  $K$  be an imaginary quadratic number field and let  $K_\emptyset$  be the maximal unramified 2-extension of  $K$ . Let  $S = \{l_1, \dots, l_n, \infty\}$  denote the set of ramified primes in  $K/\mathbb{Q}$ . A result of Koch describes the structure of  $G(K_\emptyset/K)$  in terms of generators and relations.

**Theorem 2.1.** (Koch, [Ko]) *There exists a minimal presentation*

$$1 \longrightarrow R \longrightarrow F \longrightarrow G(K_\emptyset/K) \longrightarrow 1$$

of  $G(K_\emptyset/K)$  where  $F$  is a free pro-2-group on generators  $x_1, \dots, x_{n-1}$ . The relation subgroup  $R$  is generated as a normal subgroup of  $F$  by relators  $r_1, \dots, r_n$  which are given modulo  $F_{(3)}$  by

$$r_m \equiv x_m^{2\ell_{m,n}} \prod_{\substack{1 \leq j \leq n-1 \\ j \neq m}} (x_m^2 x_j^2 (x_m, x_j))^{\ell_{m,j}} \pmod{F_{(3)}}, \quad m = 1, \dots, n,$$

$$r_n \equiv \prod_{m=1}^{n-1} (x_m^2)^{\ell_{n,m}} \pmod{F_{(3)}},$$

with

$$(-1)^{\ell_{i,j}} = \left( \frac{l_i}{l_j} \right).$$

We consider the case that  $R$  lies inside  $F_{(3)}$ . In the first section we have seen how the description of  $R$  modulo  $F_{(4)}$  is connected to triple Massey products. An arithmetic interpretation of the pairings

$$H^1(G(K_\emptyset/K)) \times H^1(G(K_\emptyset/K)) \times H^1(G(K_\emptyset/K)) \xrightarrow{(\cdot, \cdot, \cdot)} H^2(G(K_\emptyset/K)) \xrightarrow{\text{tr}} \mathbb{Z}/2\mathbb{Z}$$

(here  $H^i(G(K_\emptyset/K)) = H^i(G(K_\emptyset/K), \mathbb{Z}/2\mathbb{Z})$ ) is given by the Rédei symbol. This symbol was introduced by Rédei ([Re]) in 1934 and is defined as follows. We consider prime numbers  $p_1, p_2, p_3$  with  $p_i \equiv 1 \pmod{4}$  and

$$\left( \frac{p_1}{p_2} \right) = \left( \frac{p_1}{p_3} \right) = \left( \frac{p_2}{p_3} \right) = 1.$$

Let  $\alpha = x + y\sqrt{p_1}$ , where  $x, y \in \mathbb{Z}$  are solutions of

$$x^2 - p_1 y^2 - p_2 z^2 = 0$$

that have to fulfill some additional conditions. Then there exists a prime ideal  $\mathfrak{p}_3$  in  $k_1 = \mathbb{Q}(\sqrt{p_1})$  above  $p_3$  such that  $\mathfrak{p}_3$  is unramified in  $k_1(\sqrt{\alpha})$ , and we define the Rédei symbol  $[p_1, p_2, p_3]$  by

$$[p_1, p_2, p_3] = \begin{cases} 1, & \text{if } \mathfrak{p}_3 \text{ splits in } k_1(\sqrt{\alpha}), \\ -1, & \text{if } \mathfrak{p}_3 \text{ is inert in } k_1(\sqrt{\alpha}). \end{cases}$$

The Rédei symbol is independent of the choices we made ([Re]). We have the following theorem (see [Vo]).

**Theorem 2.2.** *Let  $K = \mathbb{Q}(\sqrt{D})$  where  $D = -l_1 \cdot \dots \cdot l_n$  with  $l_1, \dots, l_{n-1} \equiv 1 \pmod{4}$  and  $l_n \equiv 3 \pmod{4}$ , and assume that*

$$\left(\frac{l_i}{l_j}\right) = 1 \text{ for all } 1 \leq i, j \leq n, i \neq j.$$

*Then  $R \subseteq F_{(4)}$ , and for  $m = 1, \dots, n-1$  we have*

$$r_m \equiv \prod_{\substack{1 \leq i < j \leq n-1, \\ k \leq j}} ((x_i, x_j), x_k)^{e_{i,j,k,m}} \pmod{F_{(4)}},$$

*where for pairwise distinct  $i, j, k$  we have*

$$(-1)^{e_{i,j,k,m}} = \begin{cases} [l_i, l_j, l_k] & \text{if } m = j \text{ or } m = k, \\ 1 & \text{otherwise.} \end{cases}$$

*If  $\chi_1, \dots, \chi_{n-1}$  denotes the dual base of  $H^1(G(K_\emptyset/K))$  to  $x_1, \dots, x_n$ , then for the triple Massey product*

$$\langle \cdot, \cdot, \cdot \rangle : H^1(G(K_\emptyset/K)) \times H^1(G(K_\emptyset/K)) \times H^1(G(K_\emptyset/K)) \rightarrow H^2(G(K_\emptyset/K))$$

*we have (with  $i, j, k, m$  as above) the identity*

$$(-1)^{\text{tr}_{r_m} \langle \chi_i, \chi_j, \chi_k \rangle} = \begin{cases} [l_i, l_j, l_k] & \text{if } m = i \text{ or } m = k, \\ 1 & \text{otherwise.} \end{cases}$$

Since  $H^1(G(K_\emptyset/K))$  is isomorphic to  $(\text{Cl}(K)/2)^*$ , where  $\text{Cl}(K)$  denotes the ideal class group and  $*$  denotes the Pontryagin dual, we obtain pairings

$$(\text{Cl}(K)/2)^* \times (\text{Cl}(K)/2)^* \times (\text{Cl}(K)/2)^* \rightarrow \mathbb{Z}/2\mathbb{Z}.$$

**Example 2.3.** *For  $K = \mathbb{Q}(\sqrt{-5 \cdot 41 \cdot 61 \cdot 131})$  the triple Massey product considered above is nontrivial.*

## REFERENCES

- [Ko] Koch, H.: *On  $p$ -extensions with given ramification*. Appendix 1 in Haberland, K.: *Galois Cohomology of Algebraic Number Fields*, Deutscher Verlag der Wiss., Berlin, 1978
- [Mo] Morishita, M.: *Milnor invariants and Massey products for prime numbers*. *Compositio Math.* 140 (2004), 69-83
- [Re] Rédei, L.: *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I*. *J. reine u. angew. Math.* 171 (1934), 55-60
- [Vo] Vogel, D.: *On 2-extensions with restricted ramification*. to appear in *J. reine u. angew. Math.*